Non - Statutory	
Approved by	Head
Website	Y
Email	Y

ICT and Internet Acceptable Use Policy

Date Approved	October 2026
Approved by and Position	L Mathie – Head Teacher
Review Date	Autumn 2027

Policy updates

KCSIE September 2024	Released June 2024 – No changes
March 2025	5.4 – now includes 'X`
	6.2 – this has been updated to reflect the school's Behaviour and Relationship Policy
	7.2 – Policy no longer shared with parents via SchoolsComms
	Appendices – These have been renumbered and the Pupil Acceptable use information has been updated.
October 2026	Removal of names of staff who have left. Revision throughout to reflect changes to procedures and policies.

Contents

1. Introduction and aims 4
2. Relevant legislation and guidance 4
3. Definitions 5
4. Unacceptable use 6
5. Staff (including trustees, volunteers, and contractors) 8
6. Pupils 13
7. Artificial Intelligence (AI) 18
8. Parents/carers 18
9. Data security 19
10. Internet access 20
11. Monitoring and review 21
12. Related policies 21

Appendix 1 23

Appendix 2 25

Appendix 3 27

Appendix 4 29

Appendix 5 33

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including the senior leadership team), trustees, volunteers and visitors.

However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our behaviour policy / staff discipline policy / staff code of conduct.

2. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The

Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service
- **Users:** anyone authorised by the school to use the school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

- **Materials:** files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes but is not limited to:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel

- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Head Teacher / SLT will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Head Teacher's discretion.

Explain the reason to the Head Teacher
Head Teacher gives grants/denies permission
ICT Technician advised to amend the filtering software for a set period of time
ICT Technician returns filtering software to correct settings.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on behaviour / staff discipline / staff code of conduct.

5. Staff (including trustees, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

The school's ICT Technician / Business Manager / Head Teacher / SLT manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT Technician / Business Manager / Head Teacher / SLT

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Head Teacher / SLT / School Business Manager immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

The school can record incoming and outgoing phone conversations, however this is not done as a matter of course.

Staff who would like to record a phone conversation should speak to the Head Teacher/ SLT for permission and the office staff for guidance on how to do so.

All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

Examples of when permission maybe granted to record phone calls:

- Discussing a complaint raised by a parent/carer of member of the public
- Calling parents/carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments etc.
- Discussing request for term-time holidays

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Head Teacher/SLT may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching hours
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile phone policy.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of social media (see appendix 1 and the online safety policy) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts. Appendix 1.

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school

and must take such precautions as required against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

5.4 School social media accounts

The school has an official Facebook account and 'X` account, managed by designated members of staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

5.5 Monitoring and filtering of the school network and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law, is managed by EKTE with IBOS providing the filtering and Senso monitoring online use, if

anything is found then the class teacher / DSL / DDSL will speak to the pupil and parents concerned.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our trust board is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

6. Pupils

6.1 Access to ICT facilities

Laptops, Ipads, and chromebooks are available to pupils only under the supervision of staff.

Pupils will be provided unique emjoi passwords.

6.2 Searching, confiscation and deletion

Under the Education Act 2011, The Head Teacher, Assistant Head Teacher and senior members of staff have a statutory power to search pupils or their possessions, without consent, and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting has a harmful or detrimental to school discipline:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Searching with consent - Schools' common law powers to search:

School staff can search pupils **with their consent for** any item which is banned by the school rules.The school does not need to have formal written consent from the pupil/parent for this sort of search – it is enough for the teacher to ask the pupil to turn out his or her pockets or if the teacher can look in the pupil's bag and for the pupil to agree.

1. Items which are banned in school include, mobile phones, electronic games or devices.
2. If a member of staff suspects a pupil has a banned item in his/her possession, they can instruct the pupil to turn out his or her pockets or bag and if the pupil refuses, the teacher can apply an appropriate punishment as set out in the school's behaviour policy.
3. A pupil refusing to co-operate with such a search raises the same kind of issues as where a pupil refuses to stop any other unacceptable behaviour when instructed by a member of staff – in such circumstances, schools can apply an appropriate disciplinary penalty.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting behaviour which is suspected to be harmful or detrimental they should:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Head Teacher / SLT
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation if the pupil refuses to co-operate, we proceed according to the Behaviour and Relationship Policy.

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item. A list of banned items is available in the Behaviour and Relationship Policy, Appendix 2.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the Head Teacher / SLT to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the

decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Behaviour and Relationship policy
- Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute

- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. Artificial Intelligence (AI)

Our school recognises that artificial intelligence (AI), including generative AI, may be used to support teaching, learning and school activities. We are committed to ensuring that any use of AI is safe, age-appropriate, responsible and consistent with our safeguarding, online safety and data protection responsibilities.

Please see the schools safe use of AI policy for further information.

8. Parents/carers

8.1 Access to ICT facilities and materials

Parents/carers do not have access to the school's ICT facilities as a matter of course.

However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTFA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the head teacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

8.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

This policy is available on the website and on paper by request at the school office.

8.3 Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

9. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data

and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

Please see the schools cyber security policy and online safety policy for further information

10. Internet access

The school's wireless internet connection is secure.

- Filtering is provided by IBOS.
- There are 3 different WIFI connections within the school, one for pupils and staff use for educational purposes, one for guests and one for staff to connect their mobile phones to.

Filtering is not always foolproof, if a member of staff / visitor notices something which is inappropriate on the screen of a pupil. In the first instance this needs to be reported to the class teacher, this then needs to be logged to CPOMs and brought to the attention of a DSL/DDSL who can speak to the pupil / parents as appropriate and the ICT Technician who can investigate how the items has got through the filtering and where possible install fixes to stop it happening again.

10.1 Pupils

- WIFI is available across the school for pupils to use for educational purposes on school devices

- Filtering of these devices is through IBOS
- Pupils are not allowed to access the school's WIFI on personal devices.

10.2 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the head teacher.

The head teacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTFA)
- Visitors need to access the school's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)
- If staff are supporting parents/carers in submitting an application for but not limited benefits / secondary school places
- Staff must not give the WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The Head Teacher, SLT and SBM monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed on a 3 yearly basis.

12. Related policies

This policy should be read alongside the school's policies on:

- Online safety
- Cyber Security Policy
- Safe use of AI policy
- Staff code of conduct
- Safeguarding and child protection
- Behaviour and Relationship policy

- Staff discipline
- Data protection
- Remote education
- Mobile phone policy

Appendix 1

Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, make sure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster

Google your name to see what information about you is visible to the public

- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if …

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

It is at your discretion whether to respond. Bear in mind that:

- Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2

Pupil Acceptable Use Statement for EYFS and KS1 – Parent Information

Digital technologies, including mobile phones and devices which can access the internet, have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone, and they can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The school's ICT and Internet Acceptable Use Policy is intended to ensure the following:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

As your child is a member Battling Brook Community they will be expected to follow our ICT guidance and rules, and as part of their ICT lesson and our commitment to e-safety, the school will have discussed the Acceptable Use Statement with them.

All children's activity on the ICT systems will be monitored, and we take every reasonable precaution through filtering, to ensure that young people will be safe when they use the internet and ICT system. However the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet.

We ask all parents/carers to encourage their child to adopt safe use of the internet and digital technologies at home and to inform the school if they have any concerns over their child's e-safety.

The school will contact parents/carers if they have concerns about any possible breaches of the Acceptable Use Statement.

Pupil Acceptable Use Statement for EYFS and KS1

This is how I stay safe when I use computers:

- I will keep my passwords secret.
- I will only use the computer for things my teacher has told me to.
- I will make sure that all the messages I send are polite.
- I will tell a teacher if I see something that makes me feel scared or uncomfortable on the screen.
- I will not reply to any nasty message or anything that makes me feel uncomfortable.
- I will not tell people about myself online (I will not tell them my name, mobile phone number, anything about my home, family, pets and school).
- In school, I will only use my school email. I will only email people I know or who my teacher says it is okay to email.
- I know that my teacher can check what I do online and that if I break the rules I might not be allowed to use a computer.

Appendix 3

Pupil Acceptable Use Statement for KS2 – Parent information

School Policy

Digital technologies, including mobile phones and devices which can access the internet, have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone, and they can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

The school's **ICT and Internet Acceptable Use Policy** is intended to ensure the following:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.

- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

As your child is a member Battling Brook Community they will be expected to follow our ICT guidance and rules, and as part of their ICT lesson and our commitment to e-safety, the school will have discussed the Acceptable Use Statement with them.

All children's activity on the ICT systems will be monitored, and we take every reasonable precaution through filtering, to ensure that young people will be safe when they use the internet and ICT system. However the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet.

We ask all parents/carers to encourage their child to adopt safe use of the internet and digital technologies at home and to inform the school if they have any concerns over their child's e-safety.

The school will contact parents/carers if they have concerns about any possible breaches of the Acceptable Use Statement.

Pupil Acceptable Use Statement for KS2

At school we use computers, and other resources connected to the internet and our wireless network. These rules will keep us safe and help us to be fair to others.

- I will keep my passwords for login in to any computer or application to myself – if I think others know my passwords I shall tell my teacher.
- I shall use the online activities and sites which school allows me to access from home appropriately.
- I will not bring in memory sticks into school.
- I will not use my own mobile device/ phone in school unless I am given permission from my teacher.
- If the computer asks for an update, I shall check this with my teacher.
- I will only use the computer for things my teacher has told me to.
- I will not use the internet to access unsuitable material.
- The messages I send will be polite and respectful.
- I will always report anything that I feel is unkind or makes me feel unsafe or uncomfortable to my teacher. I will not reply to any nasty messages.
- In school, I will only use my school e-mail and only e-mail people my teacher has approved.
- I will always keep my personal details private (e.g my name, mobile phone number, family information, journey to school, pets, hobbies).
- I will not register my details with online activities and websites without the permission of my teacher.
- I will not share files or photos without the permission of my teacher.
- I will not copy text or pictures from the internet and pretend it is my own work.
- I understand that the school will check my computer files and will monitor the Internet sites I visit.
- I will treat computer equipment, like all school equipment, with care and respect.
- I know that if I break the rules I might not be allowed to use a computer.

Appendix 4

Acceptable use agreement for staff and Trustees.

Acceptable use of the school's ICT facilities and the internet: agreement for staff and trustees

Name:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device:

I will:

- Only use ICT systems which I have been permitted to use.
- Ensure I obtain permission prior to accessing materials from unapproved sources.
- Only use the internet for personal use during out-of-school hours, including break and lunch time.
- Only use recommended removable media and keep this securely stored.
- Only use the approved email accounts that have been provided to me when sending communications regarding school business.
- Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected.
- Only use school-owned devices for the purpose of carrying out my school responsibilities.
- Only access websites and apps that have been approved by the head teacher.
- Understand that the usage of my school-owned devices will be monitored.
- Keep my school-owned devices with me or within my sight at all times.
- Transport school-owned devices safely.
- Provide suitable care for my school-owned devices at all times.
- Only communicate with pupils and parents on school-owned devices using appropriate channels.
- Ensure I install and update security software on school-owned devices as directed by the ICT technician.
- Immediately report any damage or loss of my school-owned devices to the School Business Manager / Head Teacher and ICT technician.
- Immediately report any security issues, such as downloading a virus, to the School Business Manager / Head Teacher and ICT technician.
- Understand that I am expected to pay an excess for any repair or replacements costs where the device was damaged or lost as a result of my own negligence.

- Make arrangements to return school-owned devices to the School Business Manager / Head Teacher upon the end of my employment at the school.
- Only use personal devices during out-of-school hours, including break and lunch times.
- Ensure personal devices are either switched off or set to silent mode during school hours.
- Only make or receive calls in specific areas, e.g. the staff room.
- Store personal devices appropriately during school hours, e.g. a lockable cupboard in the classroom.
- Understand that I am liable for any loss, theft or damage to my personal devices.
- Follow the school's Social Media Policy.
- Understand that I am representing the school and behave appropriately when posting on school social media accounts.
- Ensure I apply necessary privacy settings to social media accounts.
- Participate in any relevant training offered to me, including cyber-security and online safety.
- Allow the School Business Manager in conjunction with the ICT technician and DPO to undertake regular audits to identify any areas of need I may have in relation to training.
- Employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- Deliver any training to pupils as required.
- Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the headteacher.
- Understand that my use of the internet will be monitored by the ICT technician and recognise the consequences if I breach the terms of this agreement.
- Understand that the headteacher may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network

- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote any private business, unless that business is directly related to the school
- Attempt to bypass any filtering, monitoring and security systems.
- Share school-related passwords with pupils, staff, parents or others unless permission has been given for me to do so.
- Search for, view, download, upload or transmit any inappropriate material when using the internet.
- Use personal emails to send and/or receive school-related personal data or information, including sensitive information.
- Use personal email accounts to contact pupils or parents.
- Permit any other individual to use my school-owned devices without my supervision, unless otherwise agreed by the headteacher.
- Use school-owned devices to send inappropriate messages, images, videos or other content.
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content.
- Use school-owned devices to access personal social media accounts.
- Use personal devices to communicate with pupils or parents.
- Access the school's Wi-Fi using a personal device unless permission to do so has been granted by the School Business Manager, head teacher or ICT technician.
- Use personal devices to take photographs or videos of pupils or staff.
- Store any school-related information on personal devices unless permission to do so has been given by the School Business Manager or head teacher.
- Communicate with pupils or parents over personal social media accounts.
- Accept 'friend' or 'follow' requests from any pupils or parents over personal social media accounts.
- Post any comments or posts about the school on any social media platforms or other online platforms which may affect the school's reputability.
- Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos.
- Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

Monitoring workers

I understand that:

- The school will notify employees when monitoring takes place and that the school will clearly explain what personal information of mine is collected and how it's utilised and maintained.
- Monitoring is often used for security purposes, managing employees' performance, and monitoring sickness and attendance.
- Monitoring technologies include, but aren't limited to, camera surveillance, webcams, technologies for timekeeping and keyboard activity, productivity tools, internet activity trackers, body-worn devices, and hidden audio recording.
- Personal data relating to myself which is collected from monitoring activities is securely kept and protected and isn't kept for any longer than necessary by the school.
- The school will factor in increased expectations of privacy if I work from home.
- The school will conduct its monitoring activities in a way that's fair and reasonably expected.
- The school will conduct its monitoring activities with transparency, clearly explaining how and why they process my information.
- The school will conduct its monitoring activities in a way that's accountable and compliant with UK GDPR.
- I can object to having my personal information collected and processed if the lawful basis which the school is relying on is a public task or legitimate interests based on my personal situation.
- The school may refuse to comply with the objection if they can demonstrate that the monitoring is for legitimate interests which override my interests, rights, and freedoms, or that the monitoring is for establishment, exercise, or defence of legal claims.
- Tools for monitoring workers continue to become increasingly sophisticated, and that the school will inform me if they choose to use solely automated processes for monitoring activities.
- I can access the information collected by the school by making a subject access request (SAR).
- The school will carry out a data protection impact assessment (DPIA) prior to undertaking their monitoring activities. Completing a DPIA identifies and minimises any potential risks that come with monitoring activities.

Agreement
I certify that I have read and understood this agreement and ensure that I will abide by each principle.

Signed:	**Date:**

Appendix 5

Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.

TERM	DEFINITION
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.